

WHAT IS CLAIMED IS:

1. A server apparatus provided in a home network of an IP network using a protocol that automates the management of an IP address and the transfer of a communication packet to a move destination when a terminal has moved between networks on the IP network, the server apparatus comprising:

memory means that stores information for constructing a safe communication path within an IP network in relation to the terminal; and

distribution means that distributes the information to construct a safe communication path between the terminal within an external network of a move destination and the other terminal with whom the terminal communicates.

2. The server apparatus according to Claim 1, wherein

the distribution means transfers the information to a router of an external network in which the other terminal exists.

3. The server apparatus according to Claim 1, wherein

the safe communication path is a communication path realized by a virtual private network, and the information includes set path information and security information of the virtual private network.

4. The server apparatus according to Claim 1, wherein

the distribution means distributes the information at the time of transmitting an authentication response message to a position registration request message from the terminal.

5. The server apparatus according to Claim 1, wherein

the distribution means distributes the information after receiving a communication packet from the other terminal that becomes the communication

destination.

6. A VPN system in a mobile IP network, the VPN system comprising:

- a mobile terminal;
- 5 a home authentication server provided in a home network of a user and an external authentication server provided in other external network;
- a VPN database provided in the home network; and
- 10 network apparatuses that have gateway functions of a home network, an external network, a predetermined communication host and/or an agent server therefor, wherein
- 15 the home authentication server extracts from a VPN database VPN information of a user who has requested an authentication at the time of a position registration request from a mobile terminal, and posts this VPN information to each network apparatus by using a predetermined position registration message and an
- 20 authentication response message, and
- the respective network apparatuses set a VPN path by the IP Sec. based on posted VPN information, to between the home network apparatus and the external network apparatus, between the home network apparatus and
- 25 the predetermined network apparatus, and/or between the external network apparatus and the predetermined network apparatus respectively.

7. The VPN system according to Claim 6, wherein
- 30 the authentication server and the network apparatus update VPN information cached in the authentication server and the network apparatus to new path information or rewrite the VPN information with position information linked with a position registration request based on a move of a mobile terminal, thereby to
 - 35 automatically update each VPN path between the home network apparatus and the external network apparatus, between the home network apparatus and the predetermined

network apparatus, and/or between the external network apparatus and the predetermined network apparatus, to a new VPN path based on the IP Sec. respectively.

5 8. The VPN system according to Claim 6, wherein
 the home authentication server includes:
 an AAAVPN control section that specifies a
VPN set path from the information of the external network
apparatus connected by the mobile terminal set in a
predetermined authentication request message and the
10 information of the home network apparatus of the mobile
terminal, by using a correspondence table showing a
correspondence between the VPN information of the VPN
database and a predetermined network apparatus
accommodating a communication host held by itself; and
15 an AAA protocol processing apparatus that
sets a service quality between the network apparatuses
and security information to a predetermined
authentication response message to an access network and
to a position registration message to the home network,
20 as service profiles.

 9. The VPN system according to Claim 6, wherein
 each network apparatus includes:
 an MA protocol processing section that
controls protocols relating to a service profile in which
25 the VPN information has been set by caching; and
 an MAVPN control section that sets a QoS
control for guaranteeing the service quality and a tunnel
for guaranteeing the security between the security
gateways according to the service profile.

30 10. An external authentication server existing with
a mobile terminal in an IP network using a protocol that
automates the management of an IP address and the
transfer of a communication packet to a move destination
when the terminal has moved between networks on the IP
35 network, the external authentication server comprising:
 means that extracts safety path
information corresponding to a user included in a

00001557 000001

response message from a home authentication server when the mobile terminal has made a position registration request; and

safety path construction instruction means that instructs a network apparatus accommodating the mobile terminal to construct a safe communication path between this network apparatus and a network apparatus accommodating the other terminal as a communication destination, based on the extracted safety path information.

11. The external authentication server according to Claim 10, wherein

the safe communication path is a communication path realized by a virtual private network, and the safety path information includes set path information and security information of the virtual private network.

12. The external authentication server according to Claim 11, wherein

the safe communication path is a VPN path according to the IP Sec.

13. A network apparatus for accommodating a mobile terminal in an IP network using a protocol that automates the management of an IP address and the transfer of a communication packet to a move destination when a terminal has moved between networks on the IP network, the network apparatus comprising:

means that receives a safety path construction instruction based on safety path information corresponding to a user included in a response message from a home authentication server when the mobile terminal has made a position registration request; and

safety path construction means that constructs a safe communication path between this network apparatus and a network apparatus accommodating the other terminal as a communication destination, based on the received safety path construction information.

14. The network apparatus according to Claim 13,
wherein

the safe communication path is a
communication path realized by a virtual private network,
5 and the safety path information includes set path
information and security information of the virtual
private network.

15. The network apparatus according to Claim 14,
wherein

10 the safe communication path is a VPN path
according to the IP Sec.

16. A VPN setting method in a mobile IP network
comprising the steps:

that a user network apparatus sets VPN
15 path by a stationary IP Sec. tunnel directed from the
user network apparatus to its home agent;

that a user mobile terminal transmits a
position registration request message to a foreign agent;

20 that the foreign agent transmits an
authentication request message including the received
position registration request information to a user home
authentication server via a local authentication server
of the foreign agent;

25 that, based on the received authentication
request message, the home authentication server refers to
its own database and extracts a communication destination
host, a type of the network apparatus, and security
service information by users, caches the VPN information
between the foreign agent and the home agent and between
30 the user network apparatus and the home agent, and
transmits the position registration request message
including this information to the home agent;

that the home agent caches the received
position registration request message, sets the assigned
35 security service, sets a VPN path by an IP Sec. tunnel
directed from the home agent to the user network
apparatus as a communication destination host and to the

00004557 000004
FOUO

foreign agent respectively, and transmits a position registration response message to the home authentication server after finishing the position registration processing;

that, based on the reception of the position registration response message, the home authentication server transmits the authentication response message added with the cached VPN information between the foreign agent and the home agent, to a local authentication server of the foreign agent;

that the local authentication server transmits the received authentication response message to the foreign agent after caching the VPN information between the home agent and the foreign agent; and

that the foreign agent caches the VPN information included in the received authentication response message, sets the assigned security service, sets a VPN path by an IP Sec. tunnel directed from the foreign agent to the home agent, and then returns the position registration response message to the user mobile terminal.

17. The VPN setting method according to Claim 16, further comprising the steps:

that the user mobile terminal moves to an area of a new foreign agent within the same network, and transmits from there a position registration request message including position information of the old foreign agent;

that the new foreign agent transmits an authentication request message including the received position registration request information to the local authentication server;

that the local authentication server rewrites the foreign agent information of the cached VPN information between the foreign agent and the home agent to the information of the new foreign agent, and transmits an authentication response message including

this information to the new foreign agent;

that the new foreign agent transfers the received position registration request message to the home agent;

5 that, based on the received position registration request information, the home agent rewrites the foreign agent information of the cached VPN information between the foreign agent and the home agent to the information of the new foreign agent, deletes the
10 VPN path directed from the home agent to the old foreign agent, sets a VPN path by an IP Sec. tunnel directed from the home agent set with the assigned security service to the new foreign agent, and transmits a position registration response message to the new foreign agent
15 after finishing the position registration processing; and

 that the new foreign agent caches the VPN information included in the received position registration response message, sets the assigned security service, sets a VPN path by an IP Sec. tunnel directed
20 from the new foreign agent to the home agent, and then returns the position registration response message to the user mobile terminal.

18. The VPN setting method according to Claim 16, further comprising the steps:

25 that the user mobile terminal moves to an area of a new foreign agent within a different network, and transmits from there a position registration request message including position information of the old foreign agent;

30 that the new foreign agent transmits an authentication request message including the received position registration request information to the home authentication server of the user via a local authentication server of the new foreign agent;

35 that the home authentication server rewrites the foreign agent information of the cached VPN information between the foreign agent and the home agent

2025 RELEASE UNDER E.O. 14176

to the information of the new foreign agent, and transmits the position registration request message including this information to the home agent;

5 that, based on the received position registration request information, the home agent updates the cached VPN information, deletes the VPN path directed from the home agent to the old foreign agent, sets a VPN path by an IP Sec. tunnel directed from the home agent set with the assigned security service to the new foreign
10 agent, and transmits a position registration response message to the home authentication server after finishing the position registration processing;

 that, based on the reception of the position registration response message, the home
15 authentication server transmits the authentication response message added with the cached VPN information between the foreign agent and the home agent, to a local authentication server of the new foreign agent;

 that the local authentication server
20 transmits the received authentication response message to the new foreign agent after updating the cached VPN information; and

 that the new foreign agent caches the VPN information included in the received authentication
25 response message, sets the assigned security service, sets a VPN path by an IP Sec. tunnel directed from the new foreign agent to the home agent, and then returns the position registration response message to the user mobile terminal.

30 19. A VPN setting method in a mobile IP network comprising the steps:

 that a user mobile terminal transmits a position registration request message from the user mobile terminal to a foreign agent;

35 that the foreign agent transmits an authentication request message including the received position registration request information to a user home

2025 RELEASE UNDER E.O. 14176

authentication server via a local authentication server of the foreign agent;

5 that, based on the received authentication request message, the home authentication server refers to its own database and extracts a communication destination host, a type of the network apparatus, and security service information by users, sets a VPN between the foreign agent and the communication destination network apparatus to a VPN cache when the type of the network apparatus is a one to which a VPN can be set dynamically, and transmits the position registration request message including this information to the home agent;

10 that the home agent caches the received position registration request message, and transmits a binding update message added with this VPN information to the communication destination host after finishing the position registration processing, when the type of the network apparatus is a one to which a VPN can be set dynamically;

15 that the network apparatus receives the binding update message on behalf of the communication destination host, caches the VPN information added to this message, sets the assigned security service, sets a VPN path by an IP Sec. tunnel directed from the network apparatus to the foreign agent, and thereafter transmits a binding authorization message to the home agent;

20 that, upon receiving the binding authorization message, the home agent transmits a position registration response message to the home authentication server;

25 that, based on the reception of the position registration response message, the home authentication server transmits the authentication response message added with the cached VPN information between the foreign agent and the network apparatus, to a local authentication server of the foreign agent;

30 that the local authentication server

transmits the received authentication response message to the foreign agent after caching the VPN information added to this message; and

5 that the foreign agent caches the VPN information included in the received authentication response message, sets the assigned security service, sets a VPN path by an IP Sec. tunnel directed from the foreign agent to the network apparatus, and then returns the position registration response message to the user
10 mobile terminal.

20. The VPN setting method according to Claim 19, further comprising the steps:

15 that the user mobile terminal moves to an area of a new foreign agent within the same network, and transmits from there a position registration request message including position information of the old foreign agent;

20 that the new foreign agent transmits an authentication request message including the received position registration request information to the local authentication server;

25 that the local authentication server rewrites the foreign agent information of the cached VPN information between the foreign agent and the network apparatus to the information of the new foreign agent, and transmits an authentication response message including this information to the new foreign agent;

30 that the new foreign agent transfers the received position registration request message to the home agent;

35 that, based on the received position registration request information, the home agent rewrites the foreign agent information of the cached VPN information between the foreign agent and the network apparatus to the information of the new foreign agent, and transmits a binding update message added with this VPN information to the communication destination host,

200405250000

when the type of the network apparatus is a one to which a VPN can be set dynamically;

that, based on the received binding update message, the network apparatus updates the cached VPN information, deletes the VPN path directed from the network apparatus to the old foreign agent, sets a VPN path by an IP Sec. tunnel directed from the network apparatus set with the assigned security service to the new foreign agent, and thereafter transmits a coupling authorization message to the home agent;

that, upon receiving the binding authorization message, the home agent transmits a position registration response message to the new foreign agent; and

that the new foreign agent caches the VPN information included in the received position registration response message, sets the assigned security service, sets a VPN path by an IP Sec. tunnel directed from the new foreign agent to the network apparatus, and then returns the position registration response message to the user mobile terminal.

21. The VPN setting method according to Claim 19, further comprising the steps:

that the user mobile terminal moves to an area of a new foreign agent within a different network, and transmits from there a position registration request message including position information of the old foreign agent;

that the new foreign agent transmits an authentication request message including the received position registration request information to the home authentication server of the user via a local authentication server of the new foreign agent;

that the home authentication server rewrites the foreign agent information of the cached VPN information between the foreign agent and the home agent to the information of the new foreign agent, and

transmits the position registration request message including this information to the home agent;

5 that, based on the received position registration request information, the home agent updates the cached VPN information, and transmits a binding update message added with this VPN information to the communication destination host when the type of the network apparatus is a one to which a VPN can be set dynamically;

10 that, based on the received binding update message, the network apparatus updates the cached VPN information, deletes the VPN path directed from the network apparatus to the old foreign agent, sets a VPN path by an IP Sec. tunnel directed from the network apparatus set with the assigned security service to the new foreign agent, and thereafter transmits a binding authorization message to the home agent;

15 that, upon receiving the binding authorization message, the home agent transmits a position registration response message to the new foreign agent;

20 that, based on the reception of the position registration response message, the home authentication server transmits the authentication response message added with the cached VPN information between the foreign agent and the network apparatus, to a local authentication server of the new foreign agent;

25 that the local authentication server transmits the received authentication response message to the new foreign agent after caching the VPN information added to this message; and

30 that the new foreign agent caches the VPN information included in the received position registration response message, sets the assigned security service, sets a VPN path by an IP Sec. tunnel directed from the new foreign agent to the network apparatus, and then returns the position registration response message

35

2025 RELEASE UNDER E.O. 14176

to the user mobile terminal.

22. The VPN setting method according to Claim 17 or 20, further comprising the steps:

that the new foreign agent copies the
5 cached VPN information, and transmits a binding update message added with the VPN information with the transmission origin rewritten to the old foreign agent and with the transmission destination rewritten to the new foreign agent, to the old foreign agent; and

10 that, the old foreign agent caches the VPN information of the received binding update message, deletes the VPN path directed from the old foreign agent to the home agent, sets a VPN path by an IP Sec. tunnel directed from the old foreign agent set with the assigned
15 security service to the new foreign agent, and thereafter transmits a coupling authorization message to the new foreign agent.

23. The VPN setting method according to Claim 18 or 21, further comprising the steps:

20 that the new foreign agent copies the cached VPN information when the authentication response message includes the information of the old foreign agent, and transmits a binding update message added with the VPN information with the transmission origin
25 rewritten to the old foreign agent and with the transmission destination rewritten to the new foreign agent, to the old foreign agent; and

that, the old foreign agent caches the VPN information of the received coupling update message,
30 deletes the VPN path directed from the old foreign agent to the home agent, sets a VPN path by an IP Sec. tunnel directed from the old foreign agent set with the assigned security service to the new foreign agent, and thereafter transmits a coupling authorization message to the new
35 foreign agent.

24. The VPN setting method according to Claim 19, further comprising the steps:

that the user customizes the user VPN information by making access to a database of the home authentication server by predetermined communication means, and thereby changes the communication destination to a network apparatus of the type of the network apparatus to which a VPN can be set dynamically; and

the user mobile terminal transmits a position registration request message added with a service update request, to a foreign agent.

25. The VPN setting method according to Claim 24, further comprising the steps:

that the network apparatus measures a lifetime of a communication host under its management, transmits a binding request message to the home agent that has posted the VPN information when the remaining lifetime has become less than a predetermined threshold value, and deletes the VPN information when the binding update message has not been received; and

the home agent retrieves the cached VPN information from the user mobile terminal information included in the received binding request message, transmits a binding update message when the information of the network apparatus exists, and leaves it as it is when the information of the network apparatus does not exist.